FREE SUBGROUPS OF SPECIAL LINEAR GROUPS

RUPERT McCALLUM

Abstract. We present a proof of the following claim. Suppose that n is an integer such that $n > 1$ and that k is any field. Suppose that g is an element of $\mathrm{SL}(n, k)$ of infinite order. Then the set $\{h \in \mathrm{SL}(n, k) \mid \langle g, h\rangle$ is a free group of rank two$\}$ is a Zariski dense subset of $\mathrm{SL}(n, \overline{k})$ where $\overline{k}$ is an algebraic closure of k.

Our goal in this paper is to prove the following theorem:

Theorem 1. *Suppose that n is an integer such that $n > 1$, and that k is a field, and that g is an element of $\mathrm{SL}(n, k)$ of infinite order. Then the set $\{h \in \mathrm{SL}(n, k) \mid \langle g, h\rangle$ is a free group of rank two$\}$ is a Zariski dense subset of $\mathrm{SL}(n, \overline{k})$ where $\overline{k}$ is an algebraic closure of k.*

Remark 2. *If k is an algebraic extension of a finite field, then the theorem is vacuously true, because in that case elements of infinite order do not exist. In the other cases elements of infinite order do exist.*

Remark 3. *The condition that $\langle g, h\rangle$ is a free group of rank two might at first sight seem weaker than the condition that g and h are of infinite order and that the canonical homomorphism $\langle g\rangle * \langle h\rangle \to \langle g, h\rangle$ is a monomorphism. However, in fact these two conditions are equivalent by the Nielsen-Schreier theorem.*

In [2] Theorem 1 is proved for connected simple Lie groups with $\mathbb{R}$-rank one and trivial centre.

Definition 4. *If v is a valuation on a field k then k_v denotes the completion of k with respect to the valuation v.*

The following lemma is well-known; see for example [1], Proposition 1.1:

Lemma 5 (the ping-pong lemma.)**.** *Suppose that a group G acts on a compact Hausdorff space X. Suppose that $g \in G$ has fixed points g^+, g^- and $h \in G$ has fixed points h^+, h^-. Suppose that g^+ is an attracting fixed point for g and g^- is an attracting fixed point for g^{-1}, and h^+ is an attracting fixed point for h and h^- is an attracting fixed point for h^{-1}. Suppose that $\{g^+, g^-\}$ and $\{h^+, h^-\}$ are disjoint; we do not necessarily require that the members of either pair be distinct. Then there exists an integer $N > 0$ such that $\langle g, h^N\rangle$ is a free group of rank two.*

Proof of the ping-pong lemma. Assume the hypotheses of the lemma. We may choose compact neighbourhoods N_1, N_2 of g^+, g^- respectively and compact neighbourhoods N_3, N_4 of h^+, h^- respectively, such that if $i \in \{1, 2\}, j \in \{3, 4\}$, then N_i and N_j are disjoint. There will exist an integer $N > 0$ such that, for the integers $i = 1, 2, 3, 4$ respectively, the elements g^N, g^{-N}, h^N, h^{-N} respectively map N_j into N_i whenever j is any element of $\{1, 2, 3, 4\}$. So we may conclude that if w is a nontrivial reduced word in g^N and h^N, then there will exist $i, j \in \{1, 2, 3, 4\}$ such that $N_i \neq N_j$ (because either $i \in \{1, 2\}$ and $j \in \{3, 4\}$, or $i \in \{3, 4\}$

and $j \in \{1,2\}$), and w maps N_j into N_i. Consequently g^N and h^N generate a free group of rank two. Let N_3 and N_4 satisfy the same hypotheses as before, and also choose them such that they are sufficiently small that they are both disjoint from their respective images under g and g^{-1}, and let $N > 0$ be sufficiently large that h^N maps $\overline{X \setminus N_4}$ into N_3 and h^{-N} maps $\overline{X \setminus N_3}$ into N_4. It is then possible to replace N_1 and N_2 with compact neighbourhoods N_1' and N_2' of g^+, g^- respectively, such that N_1' contains $\cup_{i=1}^{N-1} g(N_3 \cup N_4)$ and N_2' contains $\cup_{i=1}^{N-1} g^{-1}(N_3 \cup N_4)$, and the disjointness condition is still satisfied. Then g and h^N generate a free group of rank two. □

Corollary 6. *Suppose that $g, h \in \mathrm{SL}(2,k)$ for some field k and that k' is the splitting field over k for the characteristic polynomials of g and h. Suppose that g and h have no common eigenvector in $(k')^2$. Suppose that there exists a valuation v on k', such that $(k')_v$ is locally compact, such that v separates the eigenvalues of h (if g is not diagonalisable) or simultaneously separates the eigenvalues of g and h (if g is diagonalisable). Then there exists an integer N and an open neighbourhood $U \subseteq \mathrm{SL}(2,k_v)$ of h (in the strong topology on $\mathrm{SL}(2,k_v)$ induced by the topology on k_v from the valuation v) such that for all $h' \in U$ the group $\langle g, (h')^N \rangle$ is a free group of rank two.*

Proof. Suppose that g, h, k, k' and v are as in the statement of the corollary. Let $G = \mathrm{SL}(2,(k')_v) \subset M_{22}((k')_v)$ and endow G with the strong topology arising from the topology on $(k')_v$ from the valuation v. Now consider the action of G on $P^1(k_v')$, also with the strong topology. We then have a continuous action of a topological group on a compact Hausdorff space. There will exist fixed points g^+, g^- for g, and fixed points h^+, h^- for h, with the properties required by the ping-pong lemma. (If g is not semisimple then we must choose $g^+ = g^-$.) There will exist an open neighbourhood $U \subseteq SL(2,(k')_v)$ of h such that all $h' \in U$ have the requisite properties, and furthermore the proof of the ping-pong lemma may be adapted to show that we may choose U so that the same choice of integer N works for all $h' \in U$. □

Corollary 7. *Suppose that $g \in \mathrm{SL}(2,k)$ has infinite order for some field k. Then $\{h \in \mathrm{SL}(2,k) \mid \langle g, h \rangle$ is a free group of rank two$\}$ is a Zariski dense subset of $\mathrm{SL}(n,\overline{k})$ where $\overline{k}$ is an algebraic closure of k.*

Proof. Suppose that $g \in \mathrm{SL}(2,k)$ has infinite order for some field k. We may assume without loss of generality that k has finite transcendence degree over its prime subfield. Let k' be the splitting field over k for the characteristic polynomial of g. If g is diagonalisable then there exists a valuation v on k', separating the eigenvalues of g. This is because g has infinite order and so the ratio of one eigenvalue to another is not a root of unity, and in general when two nonzero elements of a field with finite transcendence degree over a prime field do not have the property that the ratio of one to the other is a root of unity, then there exists a valuation on the field in question separating them. If k has characteristic zero and some of the eigenvalues of g are transcendental over the prime subfield, then v may be chosen to be archimedean. Hence it is possible to choose v such that $(k')_v$ is locally compact. Let $h \in \mathrm{SL}(2,k)$ be such that h has eigenvalues in k separated by v and such that g and h have no common eigenvector in k^2. By Corollary 6 there exists an integer N and an open neighbourhood $U \subseteq \mathrm{SL}(2,(k')_v)$ of h such that for all $h' \in U$ the group $\langle g, (h')^N \rangle$ is a free group of rank two. The set $U \cap \mathrm{SL}(2,k)$ is nonempty and open in the strong topology arising from the topology from v, and is therefore Zariski dense in $\mathrm{SL}(2,\overline{k_v})$ and therefore

also in $\mathrm{SL}(2,\overline{k})$, since $\mathrm{SL}(2,k)$ is a Zariski connected algebraic group. Its image under the map $h \mapsto h^N$ is also open in the strong topology arising from the topology from v, and is therefore also Zariski dense in $\mathrm{SL}(2,\overline{k})$. The corollary follows. $\square$

To generalise the result to $\mathrm{SL}(n,k)$ for $n > 2$ we need to generalise Lemma 5.

Lemma 8 (the generalised ping-pong lemma.)**.** *Suppose that a group G acts on a compact metric space X with distance function d and a Radon measure μ, such that there exists some integer $N > 0$ and positive real constants c_1, c_2 such that, for every open ball B of radius r such that $0 < r < 1$, $c_1 r^N \leq \mu(B) \leq c_2 r^N$. Suppose that there exist compact sets G^+, G^-, H^+, H^- such that (1) G^+ and G^- are either disjoint or equal, and H^+ and H^- are disjoint; (2) none of these sets is contained in another one except that G^+ and G^- may be equal; (3) $\mu(G^+) = \mu(G^-) = \mu(H^+) = \mu(H^-) = 0$; (4) G^+ and G^- are fixed setwise by any power of g, and H^+ and H^- are fixed setwise by any power of h; (5) for any $x \in X \setminus G^-$, $\lim_{n\to\infty} d(g^n(x), G^+) = 0$; (6) for any $x \in X \setminus G^+$, $\lim_{n\to\infty} d(g^{-n}(x), G^-) = 0$; (7) for any $x \in X \setminus H^-$, $\lim_{n\to\infty} d(h^n(x), H^+) = 0$; (8) for any $x \in X \setminus H^+$, $\lim_{n\to\infty} d(h^{-n}(x), H^-) = 0$. Then there exists an integer $N > 0$ such that g and h^N generate a free group of rank two.*

Proof of the generalised ping-pong lemma. Given any ϵ such that $0 < \epsilon < 1$, we may choose open neighbourhoods U_1, U_2, U_3, U_4 of $(H^+ \cup H^-) \cap G^+$, $(H^+ \cup H^-) \cap G^-$, $(G^+ \cup G^-) \cap H^+$, $(G^+ \cup G^-) \cap H^-$, respectively, such that $\mu(U_i) < \epsilon$ for $1 \leq i \leq 4$. In what follows let $\{k_i\}_{i \in \{1,2,3,4\}}$ be such that $k_1 = g^N, k_2 = g^{-N}, k_3 = h^N, k_4 = h^{-N}$, and let $A_i = \{w \in \langle g^N, h^N \rangle \mid w$ has an expression as a reduced word in g and h that does not end in $k_i\}$. We may choose an integer $N > 0$ and compact neighbourhoods N_1, N_2, N_3, and N_4 of G^+, G^-, H^+, and H^- respectively, such that (1) for all i such that $1 \leq i \leq 4$, Borel sets $S \subseteq \cup_{1 \leq j \leq 4, j \neq i} N_j$, $\mu(k_i(S)) < \epsilon \cdot \mu(S)$, and (2) $g^N((N_3 \setminus U_3) \cup (N_4 \setminus U_4)) \subseteq N_1$, $g^{-N}((N_3 \setminus U_3) \cup (N_4 \setminus U_4)) \subseteq N_2$, $h^N((N_1 \setminus U_1) \cup (N_2 \setminus U_2)) \subseteq N_3$, $h^{-N}((N_1 \setminus U_1) \cup (N_2 \setminus U_2)) \subseteq N_4$. If we replace every occurence of U_i in the foregoing by $U_i' = \cup_{w \in A_i} w(U_i)$, and every occurrence of N_i by $N_i \setminus U_i'$, then $\mu(U_i')$ is still a continuous function of ϵ and as such may be made arbitrarily small. It then follows that g^N and h^N generate a free group of rank two. We may get the further conclusion that, for a sufficiently large N, g and h^N generate a free group of rank two, as in the earlier proof of the ping-pong lemma. $\square$

Proof of Theorem 1. This is as in the derivation of Corollaries 6 and 7 from the ping-pong lemma. In our application of the generalised ping-pong lemma we let the compact metric space X be $P^{n-1}((k')_v)$, where $(k')_v$ is an appropriately chosen completion of the splitting field over k for the characteristic polynomials of g and h, and we let μ be a Radon measure arising from the Haar measure on $(k')_v$ with respect to addition. We let G^+, G_-, H^+ and H^- be complementary subspaces of $P^{n-1}((k')_v)$ spanned by eigenspaces of g and h. It is possible to choose a distance function d with the desired properties. Then one may argue as in the derivation of Corollaries 6 and 7 from the table-tennis lemma to derive Theorem 1 from the generalised ping-pong lemma. $\square$

References

[1] Jacques Tits. Free Subroups in Linear Groups. *J. Alg.*, 20:250–270, 1972.

[2] Michael Cowling, M. Bekka, and P. de la Harpe. Some groups whose reduced C*–algebra is simple *Inst. Hautes Etudes Sci. Publ. Math.*, 80:117-134, 1994.